Recipe 15 - Configuration Guide for Setting up IBM Tivoli Federated Identity Manager 5.1.1 as an AA and CS

Table of Contents:

Version 2.0.0

1 Setup

1.1 Terms and Introduction

The SAML 1.0 is one of the adopted schemes within the E-Authentication architectural framework. This guide should help you setup SAML 1.0 and IBM Tivoli Federated Identity Manager 5.1.1 as an Agency Application (AA) and Credential Service (CS). Remember that the setup screens are often the same, whether setting up an AA or a CS. After reviewing the terms, configure your scheme to handle SAML 1.0, starting at the login screen shown in Figure 15-1.

Term	Definition
Agency Application (AA)	An online service provided by a government agency that requires an end user to be authenticated.
Credential Service (CS)	A service of a CSP that provides credentials to subscribers for use in electronic transactions. If a CSP offers more than one type of credential, then each one is considered a separate CS.
Credential Service Provider (CSP)	An organization that offers one or more CSs. Sometimes known as an Electronic Credential Provider (ECP).
Project Management Office (PMO)	The PMO is the organization that handles E-Authentication program management, administration, and operations.

2 Partner Configuration

2.1 Configure a Partner CS

2.1.1 Login

Open IBM Tivoli Federated Identity Manager 5.1.1. Once the application has opened, the login screen will appear as shown in Figure 15-1. Enter a valid User ID and Password and click the **Login** button.

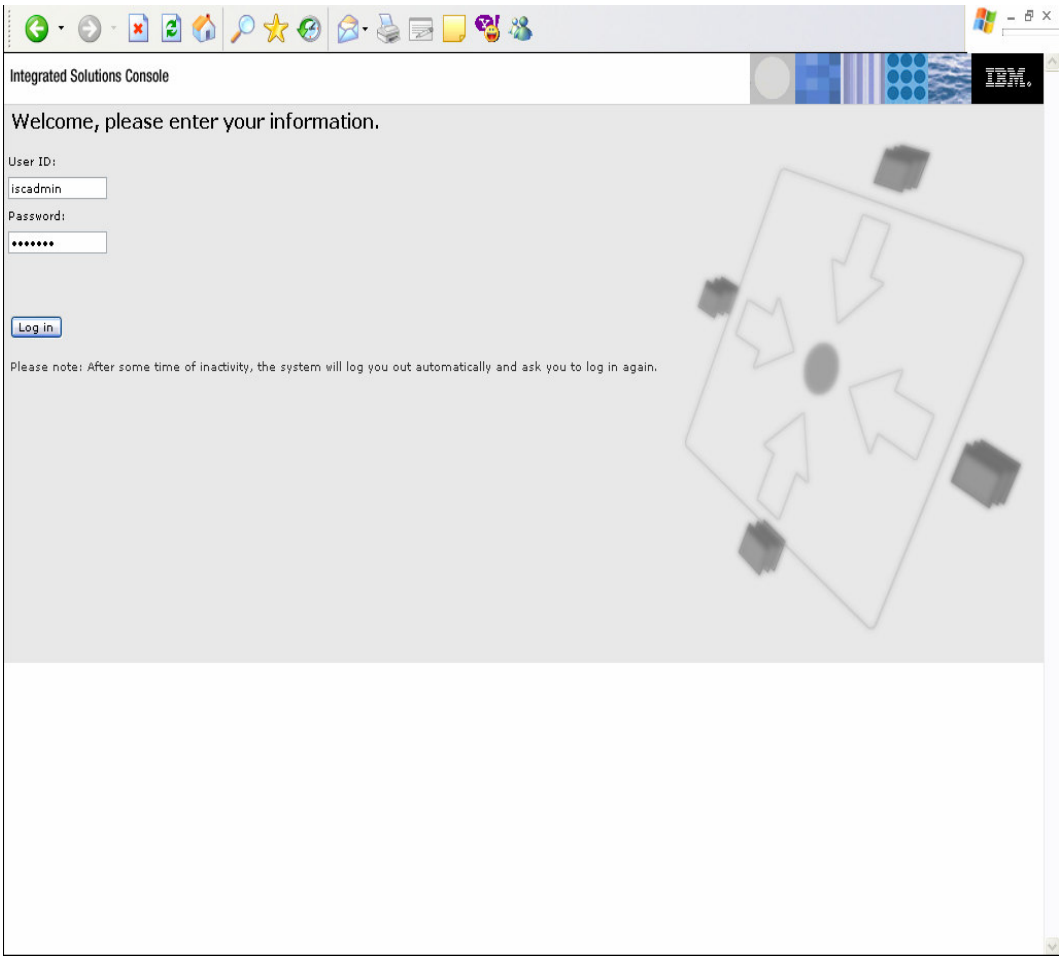

Figure 15-1: Login Screen

Once you have successfully logged into IBM Tivoli Federated Identity Manager, the Integrated Solutions Console screen will appear as shown in Figure 15-2.

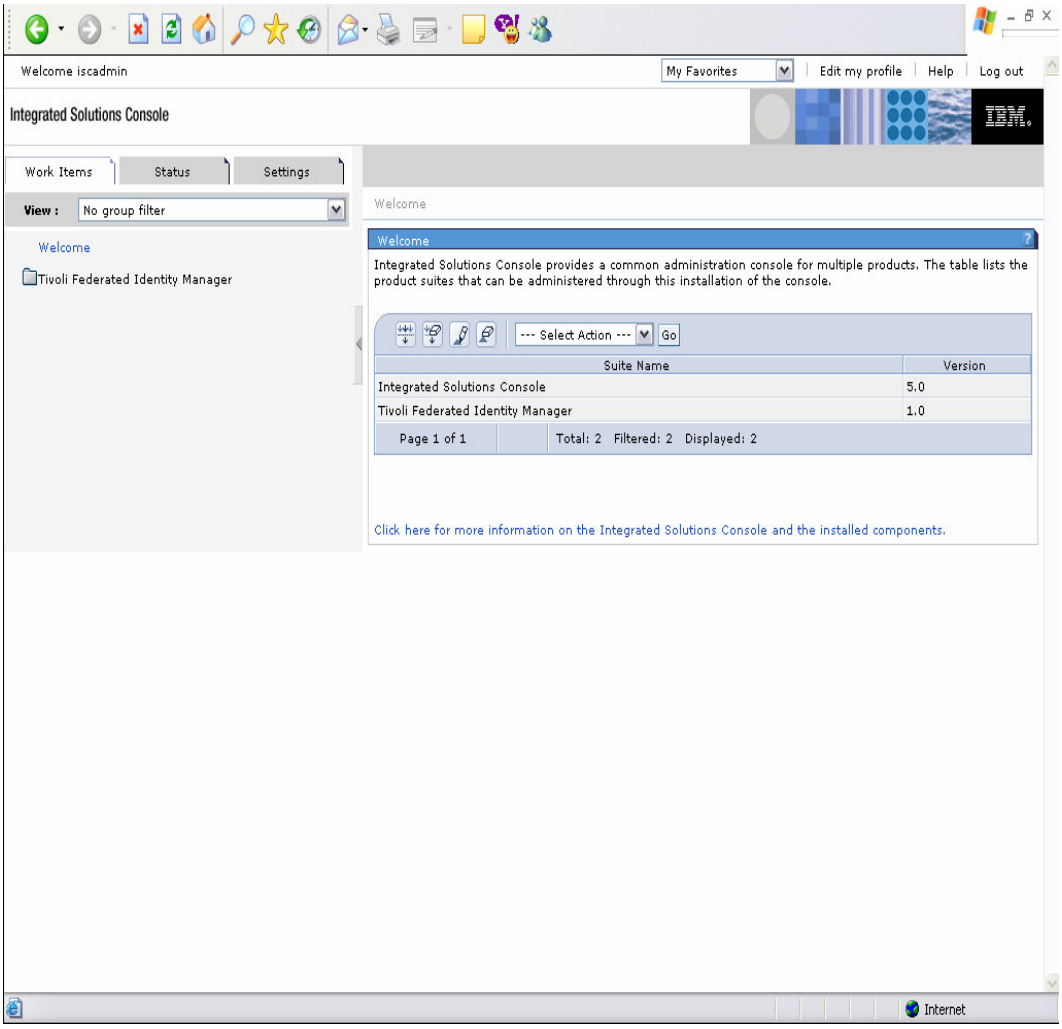

Figure 15-2: Integrated Solutions Console Screen

2.1.2 View Existing SAML Partners

It is recommended to view the existing SAML partners before starting the configuration process. This can be completed by going to the left hand side of the screen and clicking on the **Tivoli Federated Identity Manager** folder **> Federation Management > Manage Existing Federation Partners**. The existing SAML partner screen will appear as shown in Figure 15-3.

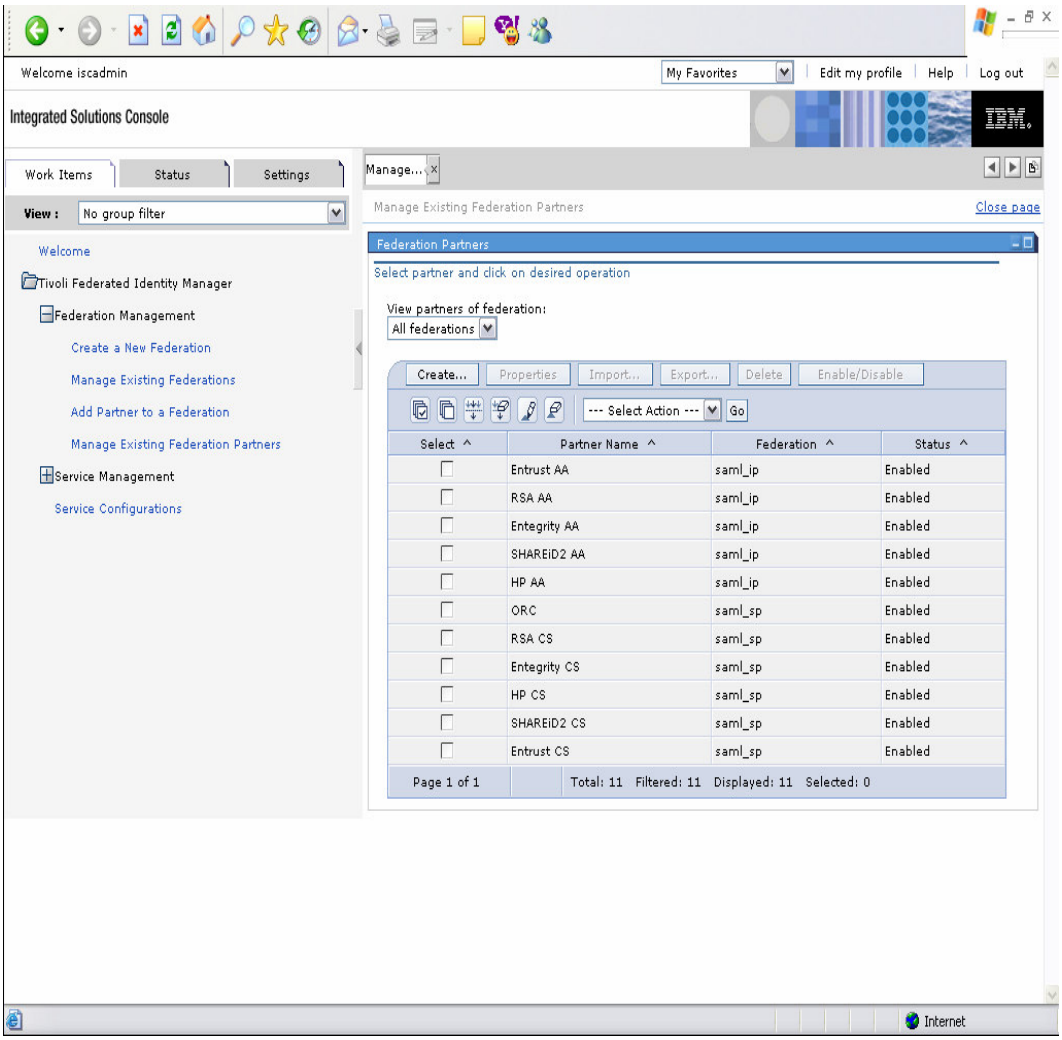

Figure 15-3: Existing SAML Partner

After viewing the existing SAML partners, open the Select Federation screen to start the configuration process. This can be completed by going to the left side of the screen and clicking on **Tivoli Federated Identity Manager > Federation Management > Add Partner to a Federation**. The Select Federation screen will appear as shown in Figure 15-4

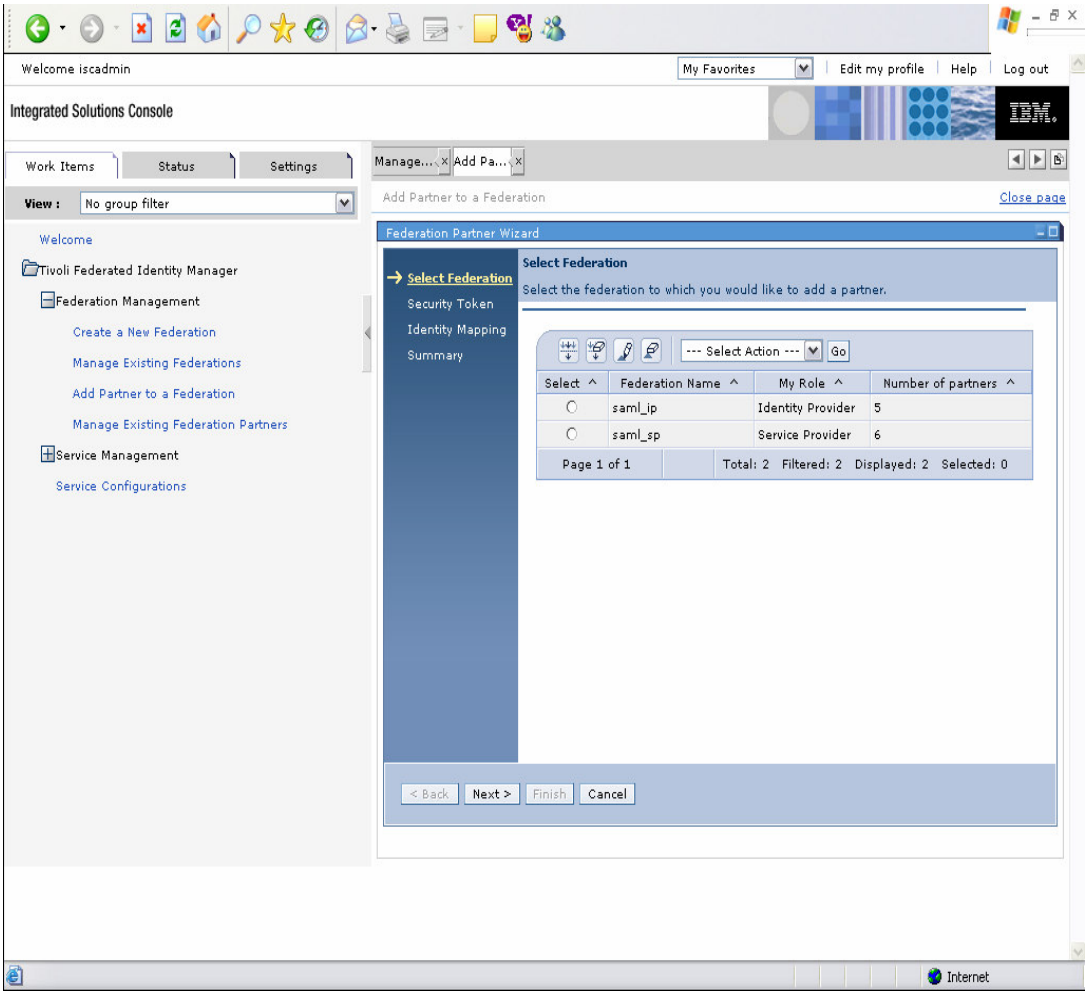

Figure 15-4: Select Federation

Next, select the federation to add a partner to (saml_ip) as demonstrated in Figure 15-5, and then click the **Next** button.

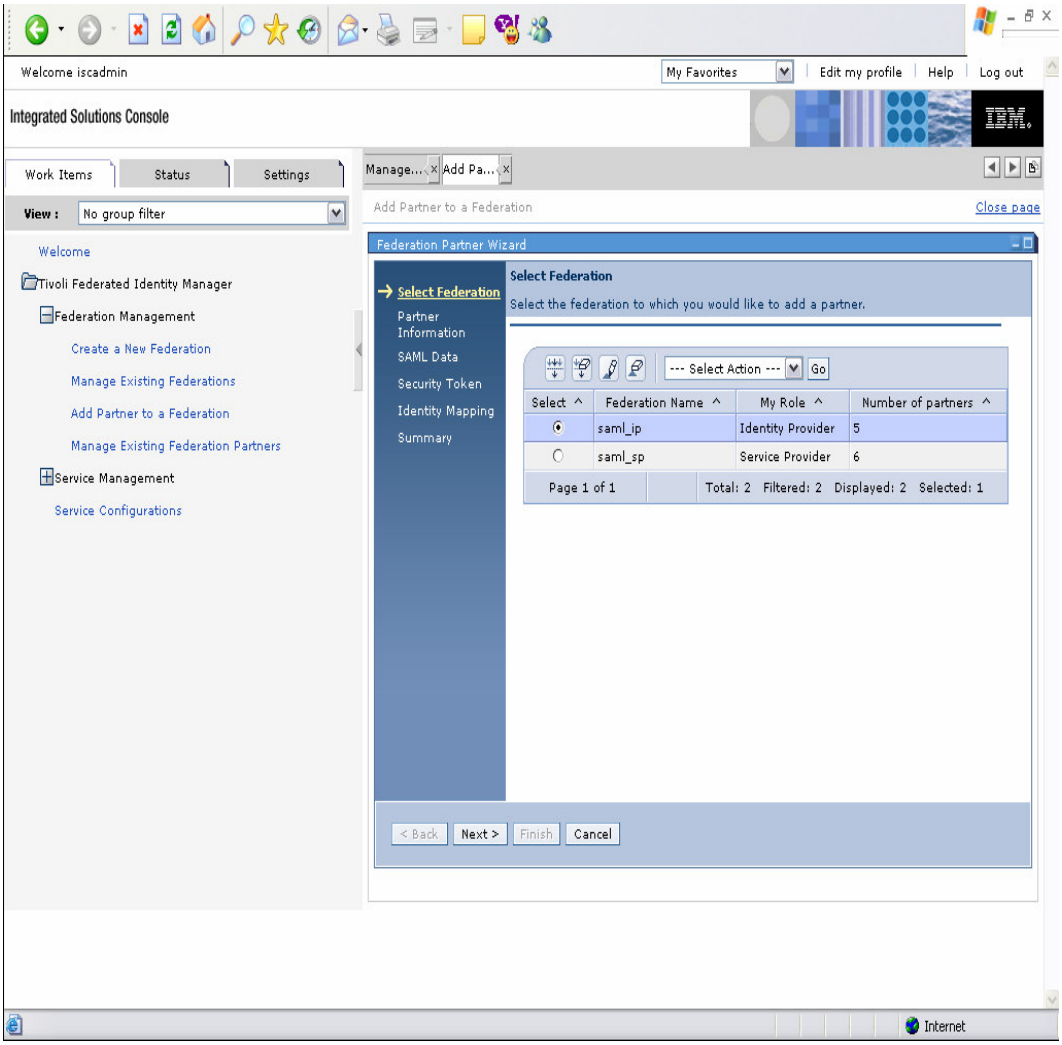

Figure 15-5: Select Federation

The Partner Information screen will appear as shown in Figure 15-6. Enter a name for the **Service Provider Company Name** (e.g. Oblix – not important) and click the **Next** button.

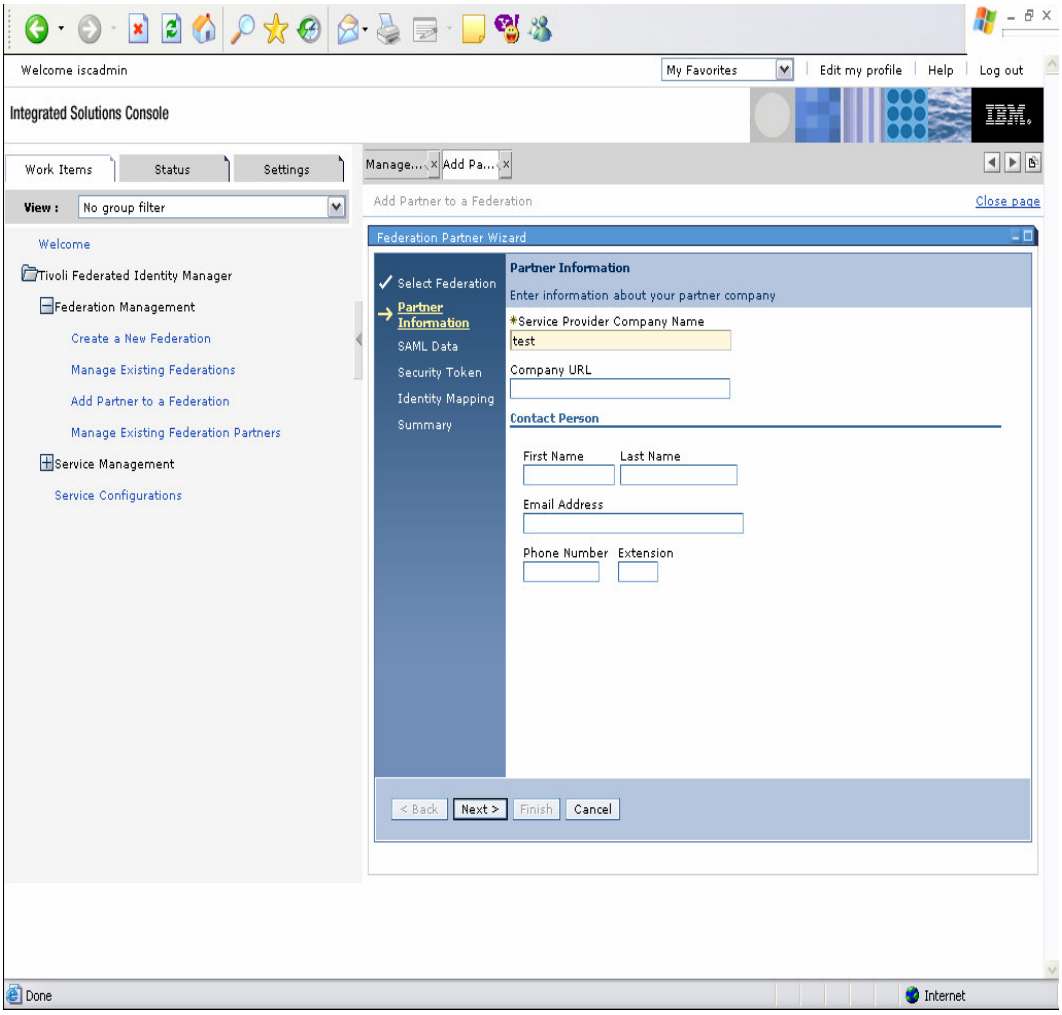

Figure 15-6: Partner Information

The SAML Data screen will appear as shown in Figure 15-7. The **Provider ID** must match the protocol://hostname[:port] of the TARGET URL for the Agency Application on the SP. The **Assertion Consumer Service URL** is also known as the "Receiver URL", which is where ITFIM will redirect the browser to with the artifact. Click on the **Next** button.

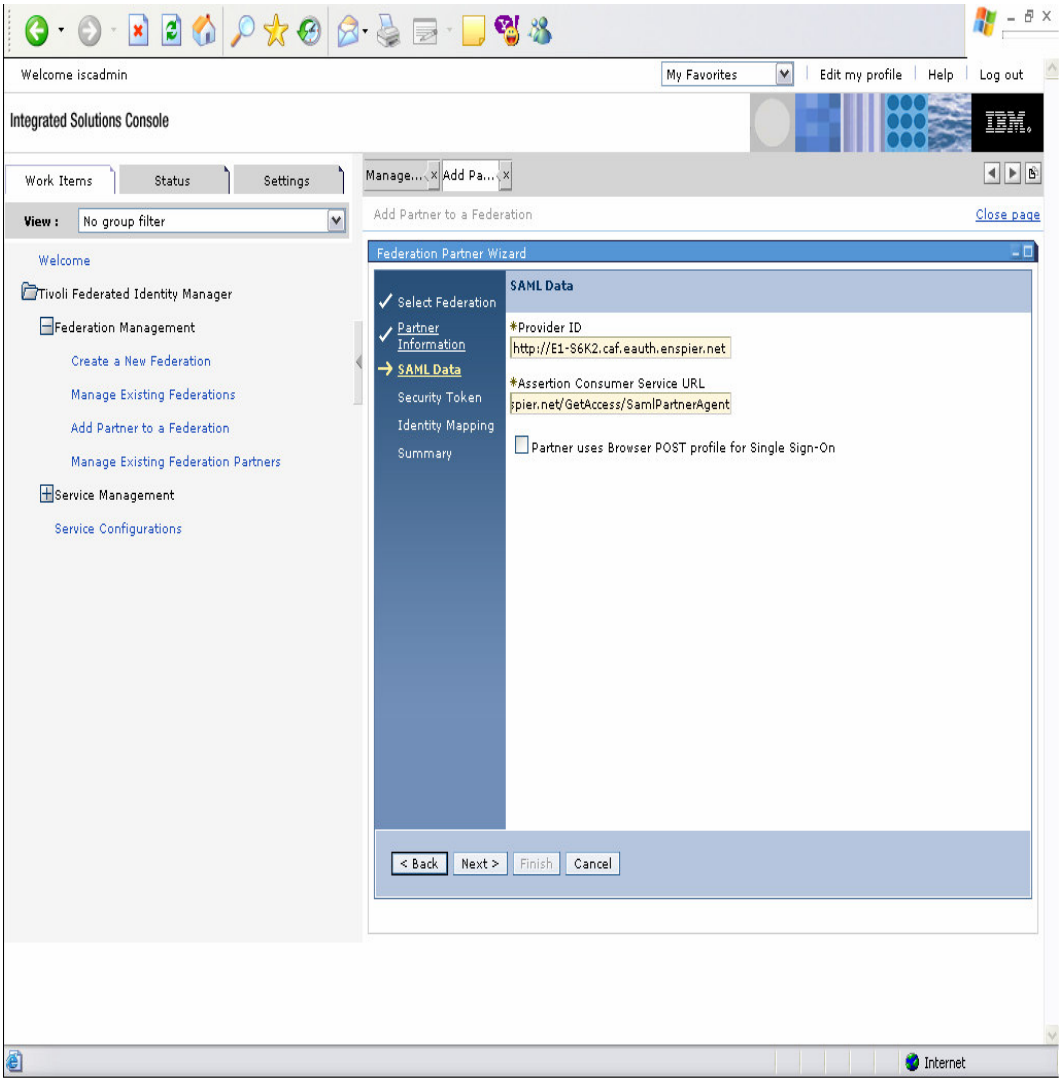

Figure 15-7: SAML Data

The default Identity Mapping screen will appear as shown in Figure 15-8. Click on the **Next** button.

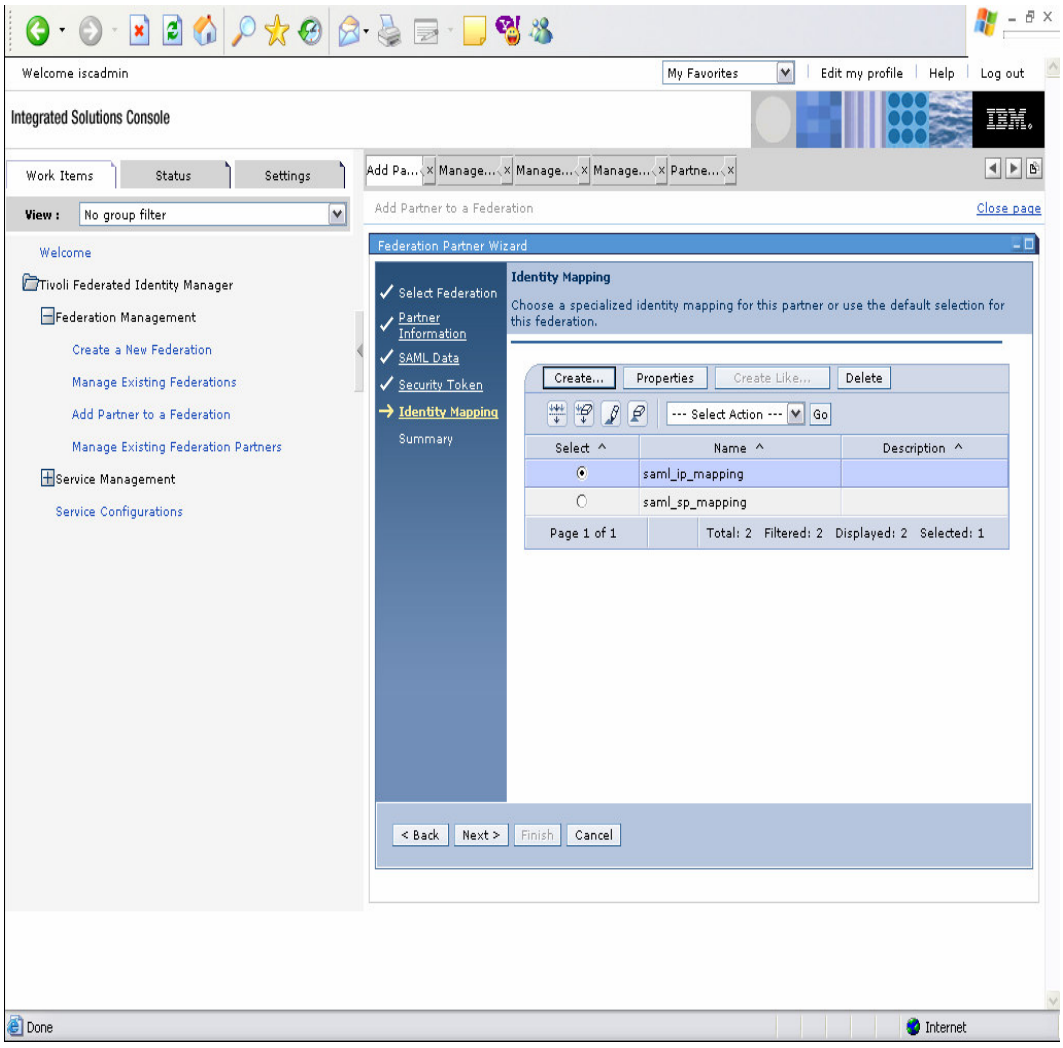

Figure 15-8: Identity Mapping

The default Security Token screen will appear as shown in Figure 15-9. Click on the **Next** button.

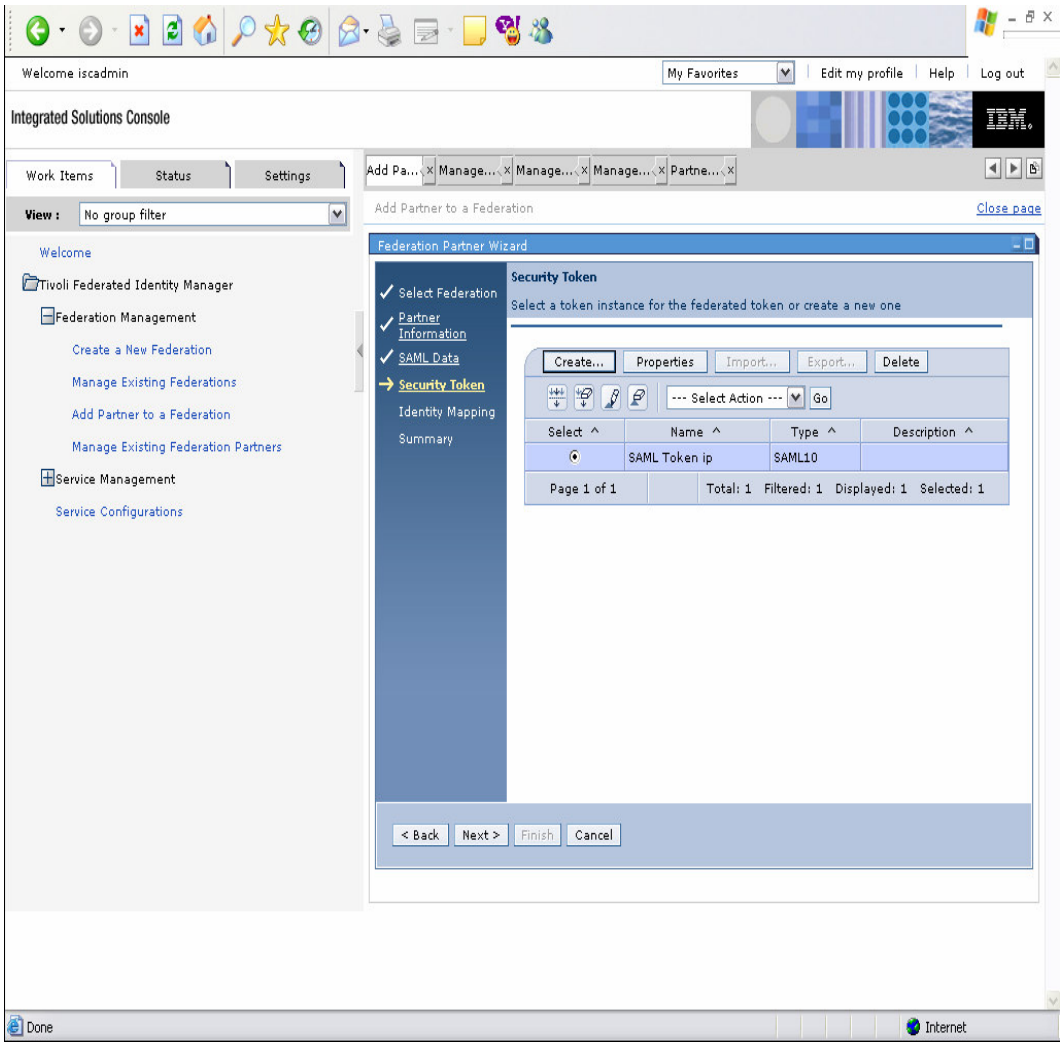

Figure 15-9: Security Token

The Summary screen will appear as shown in Figure 15-10. Be sure to check that the **Succinct Provider ID** is correct for the SAML partner you are adding. If it is not correct, you will have to manually edit the Tivoli config file. In the file /opt/Tivoli/fim/sps/etc/feds.xml search for the **Succinct ID** displayed in the summary and replace it with what the partner is going to use. If you do need to hand-modify the Succint ID, a restart of WebSphere will be required for the change to take effect. This can be accomplished by running # /opt/WebSphere/AppServer/bin/stopServer.sh server1 and
/opt/WebSphere/AppServer/bin/startServer.sh server1. Click on the **Finish** button when complete.

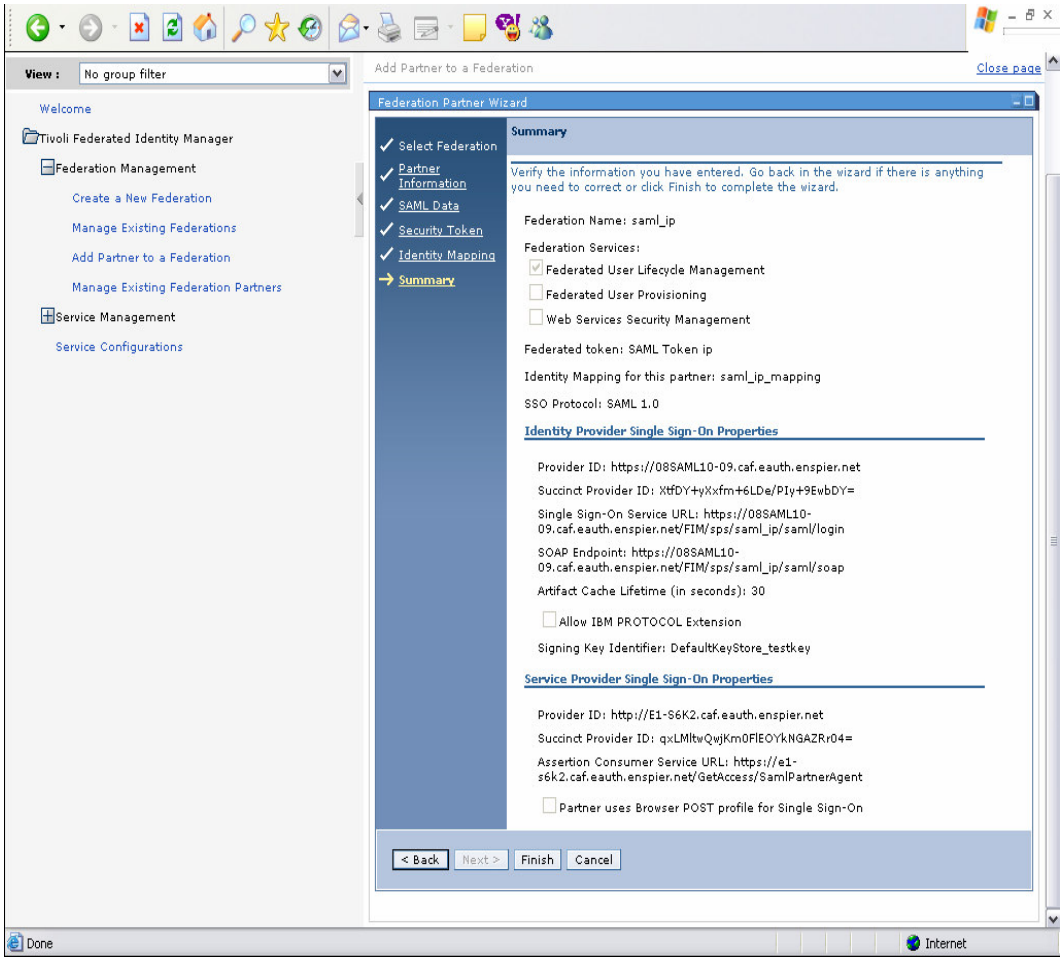

Figure 15-10: Summary

2.1.3 Create a Tivoli Access Manager

Next, you need to create a Tivoli Access Manager (TAM) user with a DN matching the DN of the client certificate that the partner is using for the mutually-authenticated SSL soap connection.

To do that, create all but the leaf node of the certificate DN in LDAP (using ldif or a preferred LDAP tool), then use our TAM administration tool to add the user. Example:

```
# pdadmin -a sec_master -p passw0rd
pdadmin> user create ibmclient "cn=fimdemo.ibm.com,ou=tameb,o=tivoli,c=us" ibmclient ibmclient passw0rd
pdadmin> user modify ibmclient account-valid yes
```

Where "cn=fimdemo.ibm.com,ou=tameb,o=tivoli,c=us" is the cert subject, and ibmclient is the alias for the cert.

You can also use the PD-WPM console for doing this at: http://hostname:9080/pdadmin

You can verify if this is successful by loading the certificate into a browser and accessing https://hostname_of_webseal and presenting the certificate for authentication.

2.2 Configure a Partner AA

2.2.1 Login

Open IBM Tivoli Federated Identity Manager 5.1.1. Once the application has opened, the login screen will appear as shown in Figure 15-11. Enter a valid User ID and Password and click the **Login** button.

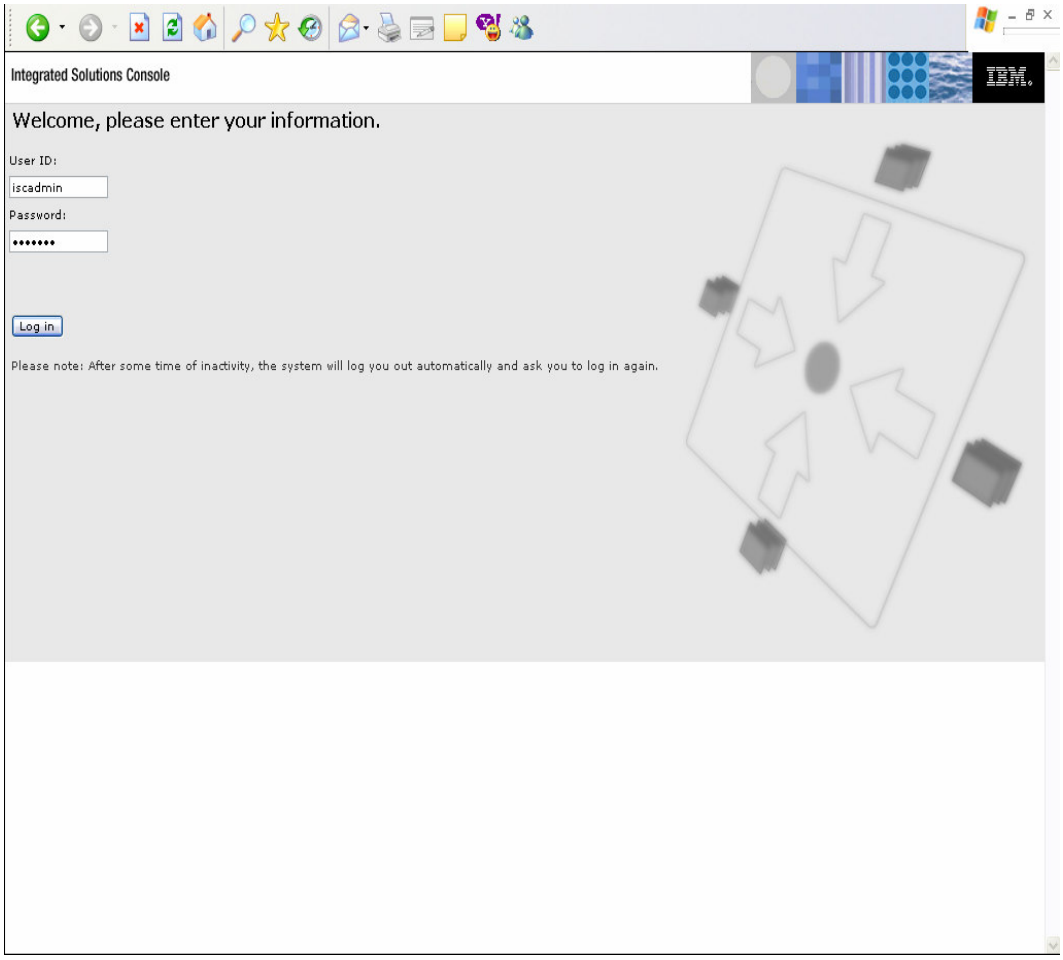

Figure 15-11: Login Screen

Once you have successfully logged into IBM Tivoli Federated Identity Manager, the Integrated Solutions Console screen will appear as shown in Figure 15-12.

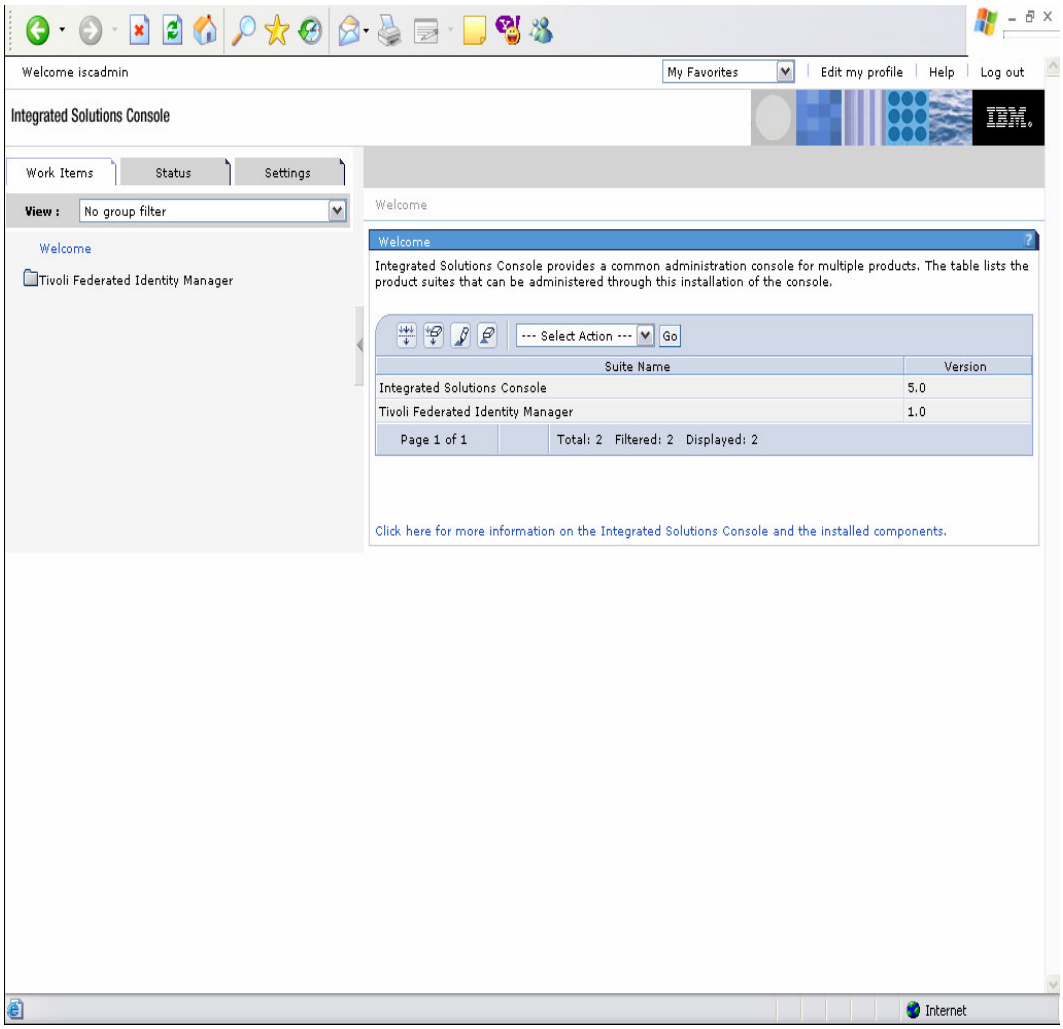

Figure 15-12: Integrated Solutions Console Screen

To add an IP Partner open the Select Federation screen by going to the left side of the screen and clicking on **Tivoli Federated Identity Manager > Federation Management > Add Partner to a Federation**. The Select Federation screen will appear as shown in Figure 15-13.

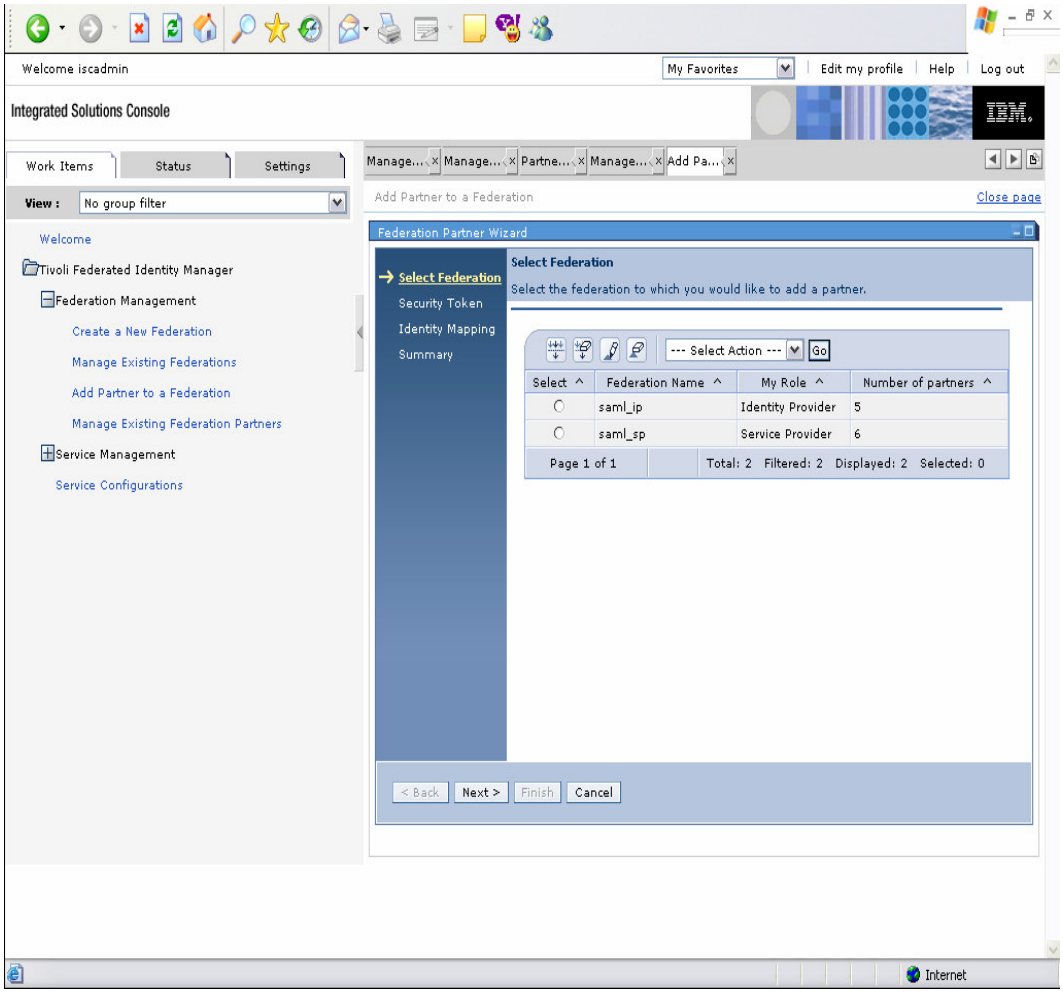

Figure 15-13: Open Select Federation Screen

Next, select the federation to add a partner to (saml_ip) as demonstrated in Figure 15-14 and then click the **Next** button.

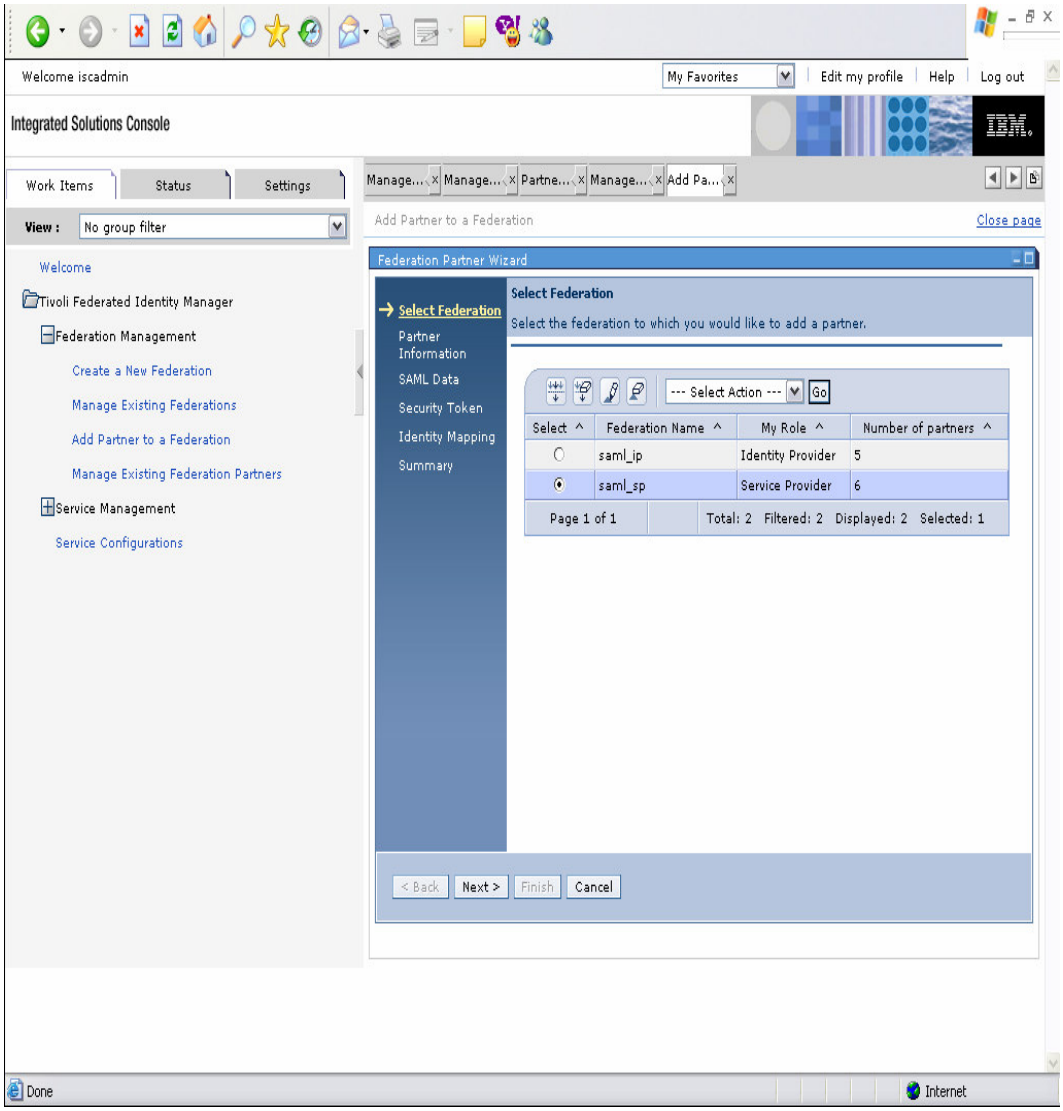

Figure 15-14: Select the Federation

The Partner Information screen will appear as shown in Figure 15-15. Enter a name for the **Identity Provider Company Name** (e.g. Oblix – not important) and click the **Next** button.

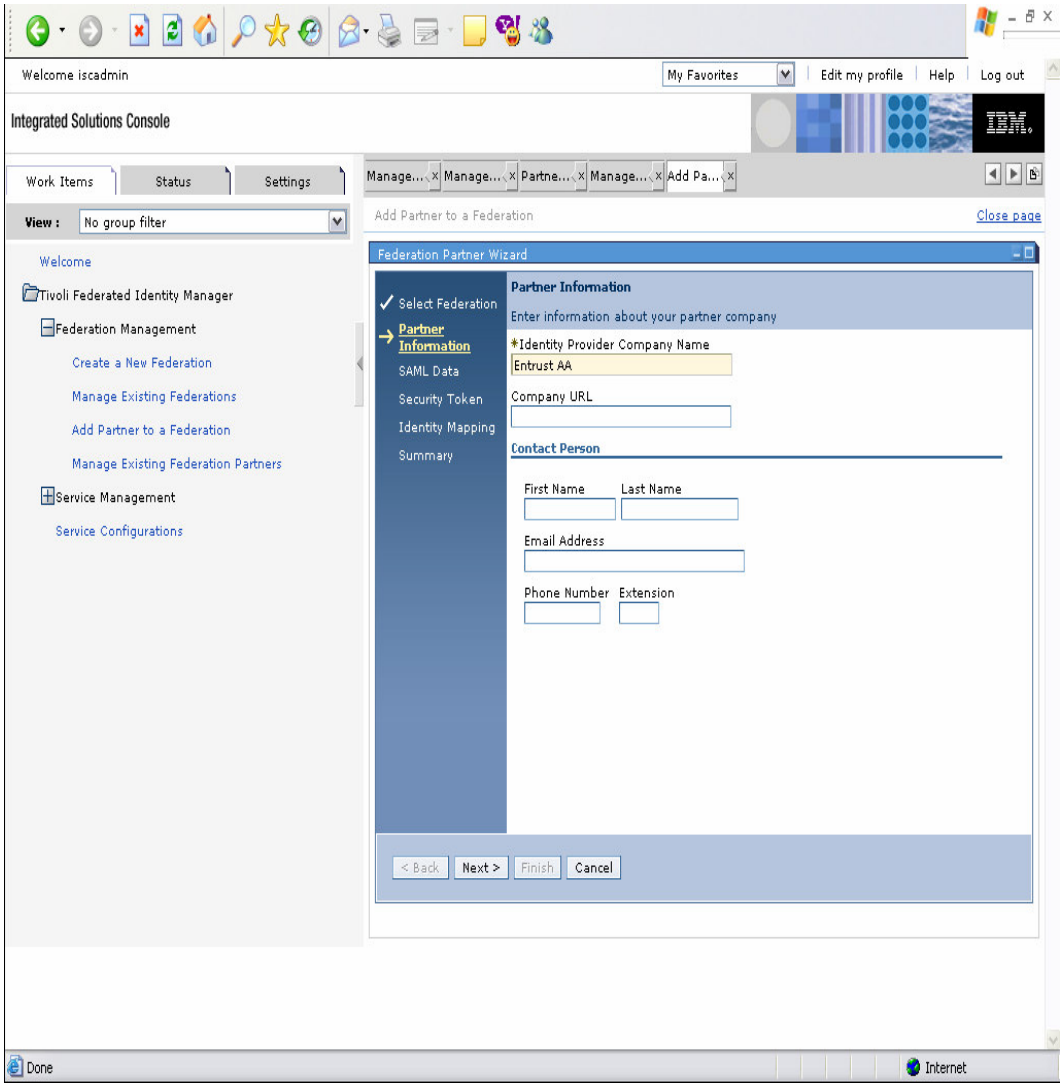

Figure 15-15: Partner Information

The SAML Data screen will appear as shown in Figure 15-16. The "**Provider ID**" must match the "Issuer" value that will appear in the SAML Assertion from the IP. The **Single Sign-on Service URL** is not important in the current version of the software (not yet used for anything), but for accuracy set it to the value of the SSO endpoint of the IP partner. The **SOAP Endpoint** is the URL of the Identity Provider that the SP will use for exchanging the artifact for an assertion. This is also known as the "Responder URL". The **Signing Key Identifier** is not used (only for Browser-POST profile) so leave it at the default.

Next, use your predefined certificate for the **SOAP *Server* Authentication Key Identifier**, select the "**Use Client Certificate for SOAP**" checkbox, enter your predefined certificate for the **SOAP *Client* Authentication Key Identifier**, enter the **password** for the **SOAP Client Authentication Key Password**, and then click the **Next** button.

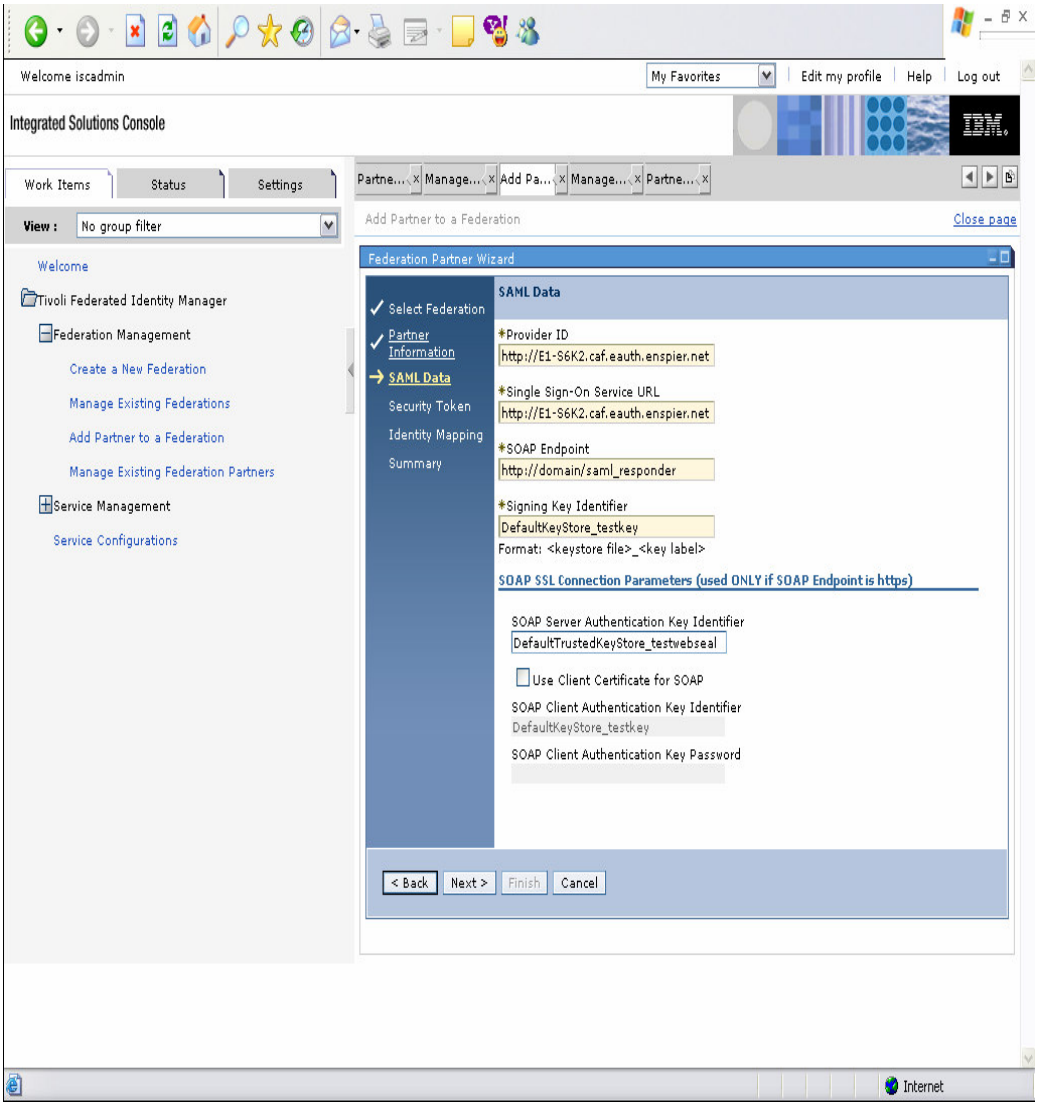

Figure 15-16: SAML Data

The Security Token screen will appear as shown in Figure 15-17. Click the **Next** button.

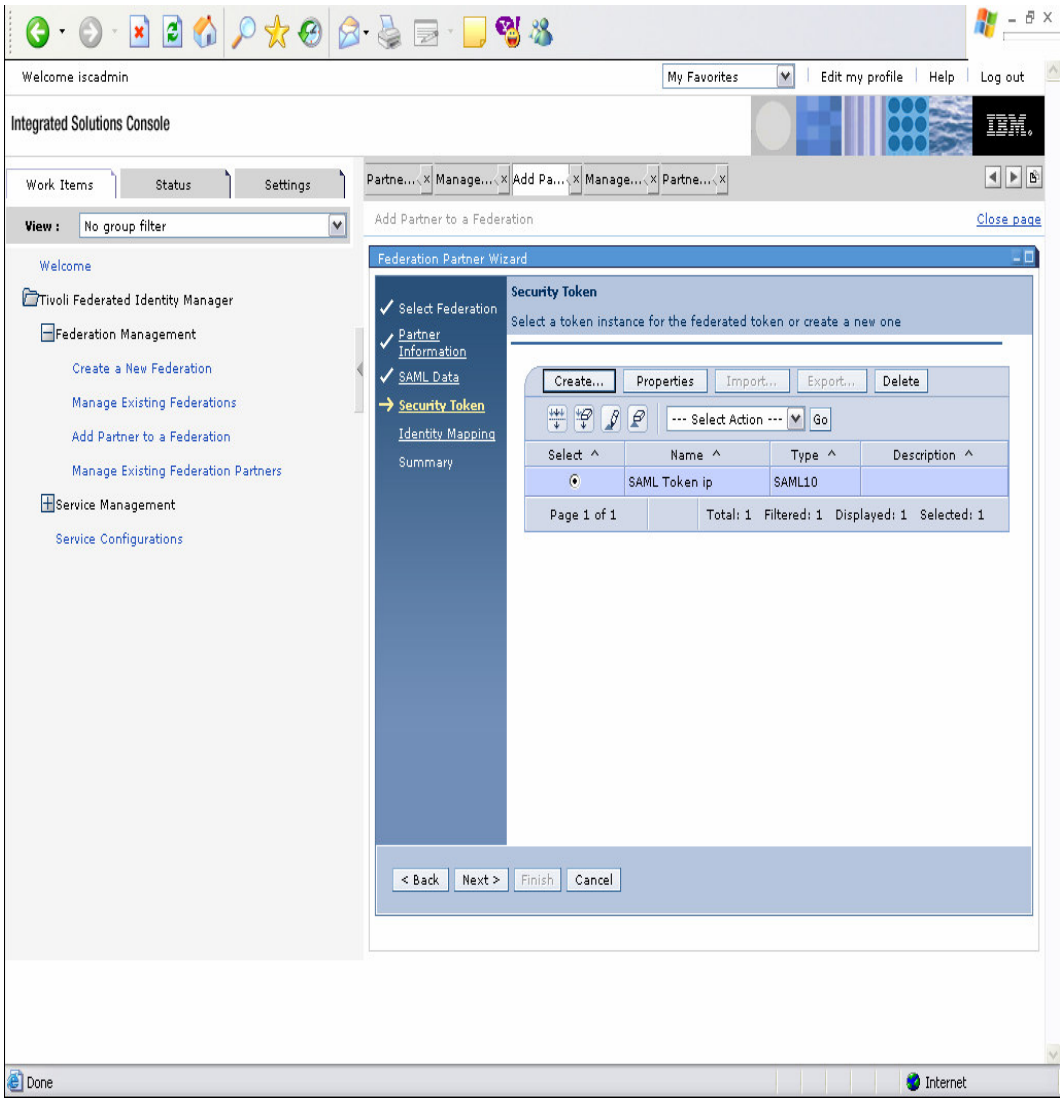

Figure 15-17: Security Token

The Identity Mapping screen will appear as shown in Figure 15-18. Click on the **Next** button.

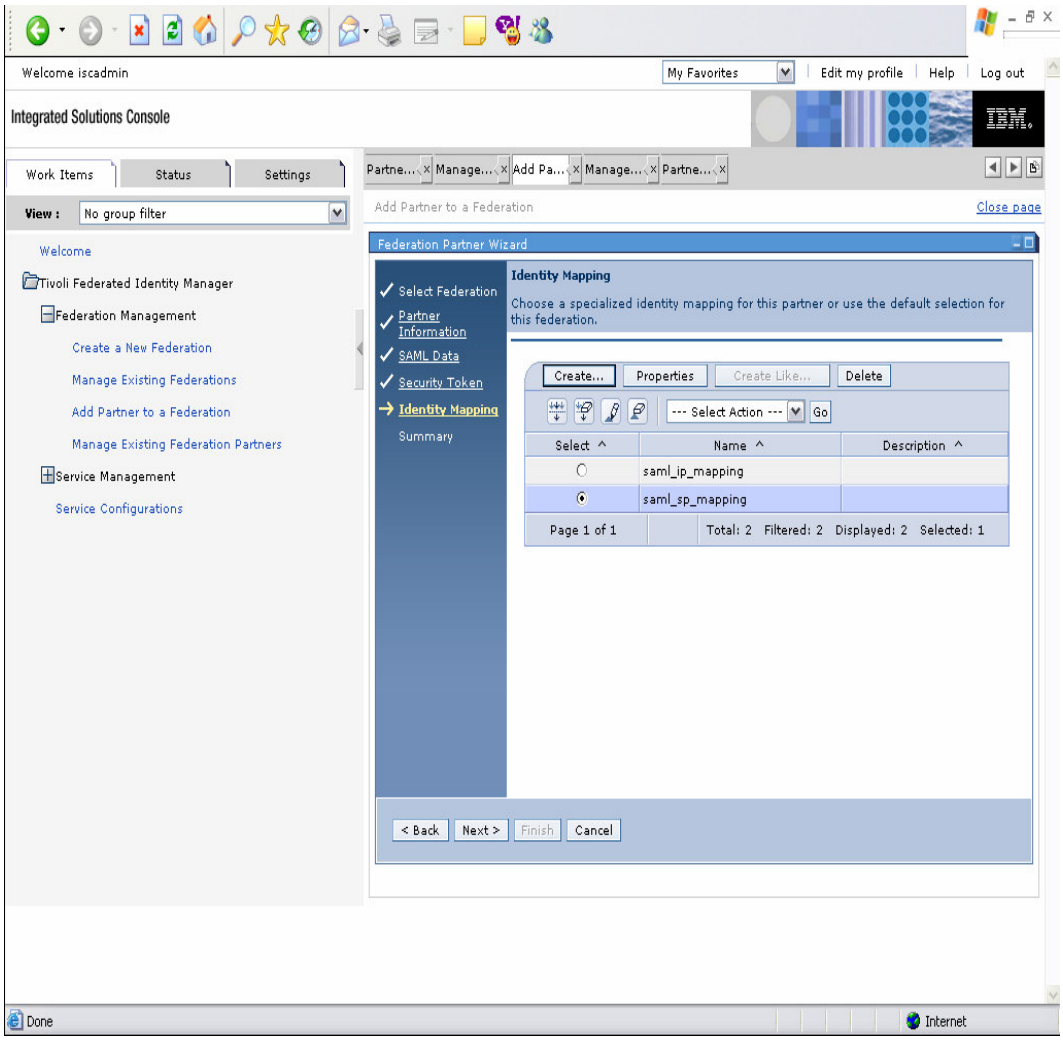

Figure 15-18: Identity Mapping

The Summary screen will appear as shown in Figure 15-19. Note the "**Succint Provider ID**" displayed for the IP partner. The ITFIM software generates this value (also known as "SourceID") from the Provider ID entered in the previous configuration page. If it does not match the SourceID value that the IP is going to set in the artifact, then you will need to hand-modify the ITFIM config files to update this.

Click on the **Finish** button to save the federation. Then, in the file /opt/Tivoli/fim/sps/etc/feds.xml search for the Succinct ID displayed in the summary and replace it with what the partner is going to use. If you do need to hand-modify the Succint ID, a restart of WebSphere will be required for the change to take effect. This can be accomplished by running # /opt/WebSphere/AppServer/bin/stopServer.sh server1 and # /opt/WebSphere/AppServer/bin/startServer.sh server1.

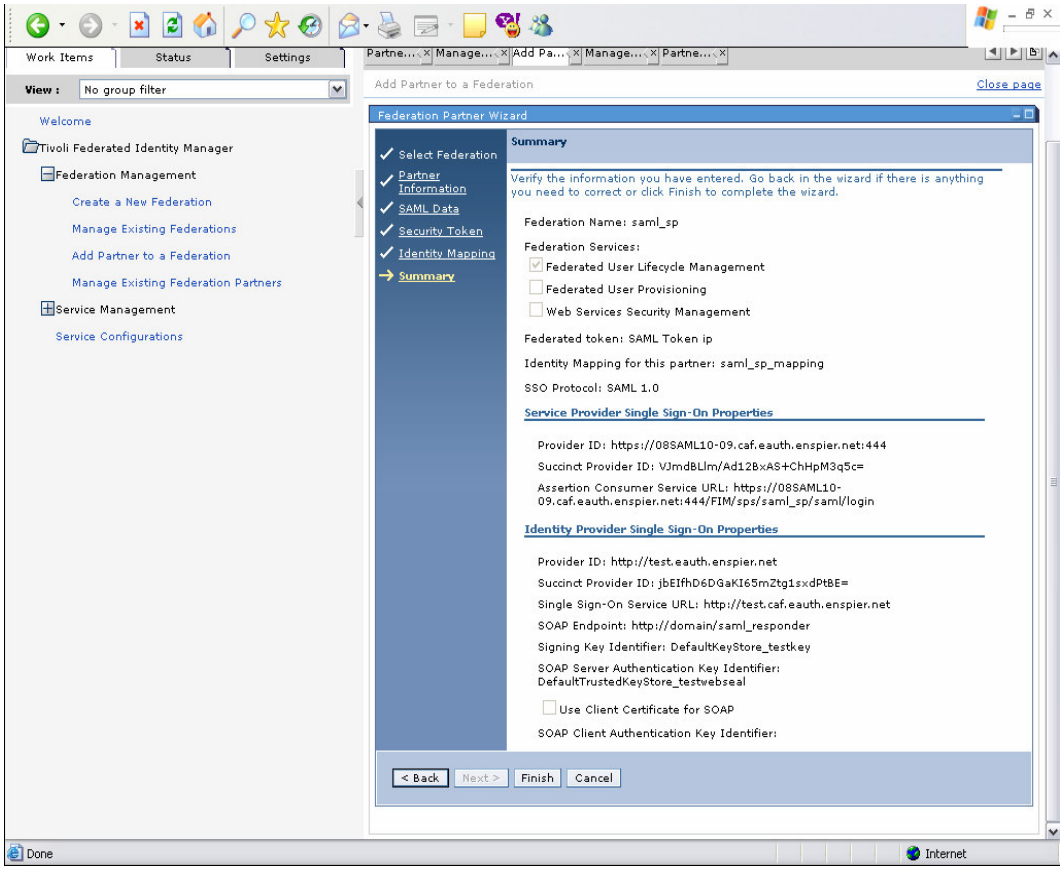

Figure 15-19: Summary